DARPA-BAA-15-56
XD3
Frequently Asked Questions

As of September 30, 2015

Q37: As mentioned on page 13 of the BAA, “Proposals for TA1, TA2, TA3 and TA5 should include two separate, optional efforts (one for the end of each phase) associated with possible participation in XD3 field exercises. The exact nature, dates and locations of these exercises will not be determined until after XD3 program commencement. Given this uncertainty, proposals should reflect a nominal two-week effort by two personnel, along with associated travel, to San Diego, CA.” Is this two-week effort per exercise (i.e., we should budget for separate two-week efforts for the two exercises) or this is the total effort for both exercises and should be split between the two separate efforts?

A37: It is a two week effort per exercise.

As of September 15, 2015

Q36: The BAA mentions Hadoop. Can proposals assume any solution that ensures distributed computations can be carried out while under attack can be included in TA1?

A36: Yes.

Q35: For TA1, can proposals include distributed monitoring modules as part of our solution?

A35: Yes.

Q34: Earlier in the FAQ it is indicated that the defense technology should reside in end points and enclaves. Do we need to consider a solution that will work with moving enclaves with wireless connectivities (apart from typical wired internet connectivity)?

A34: Consideration of wireless networks and mobility are within scope for the program, but proposers are not required to consider these cases. Proposals should clearly state what types of networks their solutions cover.

Q33: It seems that any kind of hands-on adversarial testing is not in scope for TA5. The role of the TA5 performer is simply to review the test plans and designs of the TA1-3 and 4 solutions from an adversarial perspective and provide reports, but not to stress-test them, black/white-box test them, or try to break them in any hands-on evaluation exercise. Is this an accurate interpretation?

A33: Yes.

Q32: The BAA states that this is a collaborative effort -- How will you handle the IP (we have a couple of patents) aspects of what will be developed collaboratively and what the participants bring?

A32: Per the BAA, proposers are responsible for identifying any IP licensing restrictions that are less than unlimited, as well as documenting how the Government will be able to reach its program goals (including transition) within the proprietary model. If the proposer does not make a compelling case how their proprietary solution fits within the program's collaborative and transition goals, this may be judged as a weakness in the proposal and it may not be selected. Selected performers will establish associate contractor agreements prior to kick-off, delineating what data will be shared between performers so separately developed components can be successfully integrated.

Q31: Can DARPA propose the range of the contract / grant to be considered?

A31: DARPA has no specific expectation for the cost of proposed efforts. Their cost should be realistic with respect to the scope and extent of the proposed technical work, per the BAA's Cost Realism evaluation criterion (BAA p. 34).

Q30: Traffic analysis is a component of attack detection in AT&T, both netflow and deep packet inspection. Innovations related to command and control disruption seem to be excluded from the XD3 scope. Is this view accurate?

A30: Traffic analysis, attack detection, and deep packet inspection are not within the scope of XD3 unless these functions are part of a broader solution that directly addresses one of the three program technical concepts of dispersion, networked maneuver, and adaptive endpoint sensing and response. Protection of transactional services such as those associated with military command and control are within the scope of XD3.

Q29: Page 36 of the BAA states "Proposers should note that the Government does not own the intellectual property of technical data/computer software developed under Government contracts; it acquires the right to use the technical data/computer software. Regardless of the scope of the Government's rights, performers may freely use their same data/software for their own commercial purposes". Is a more general external resource that that documents this policy?

A29: Reference DFARS Part 227 – Patents, Data, and Copyrights.

Q28: Page 19 of the BAA states “While proposers may submit proposals for all XD3 Technical Areas, performers in TA5 cannot also be performers for any portion of other TAs, whether as a prime, subcontractor, or in any other capacity from an organizational to individual level”. Would a large organization be permitted to submit multiple proposals to TA1-TA3 along with a proposal to TA5?

A28: Submit proposals: Yes. Be selected for TA1-TA3 and TA5: No.

Q27: Would our proposal be negatively affected if we require minimal implementation standards of the protected systems?

A27: Not necessarily, but proposals should clarify what they assume about the systems being protected.

Q26: Who are we defending and who is attacking?

A26: The program makes no specific assumptions about the ownership of the cyber infrastructure to be protected, or about the identity or nature of the attackers.

Q25: Is hardware offload for DDoS-exploitable protocol processing functions in scope or will a hardware requirement reduce the value of the proposal?

A25: Solutions that do not require additional and/or specific hardware requirements are preferred.

Q24: How many of the TAs 1 to 3 need to be integrated in TA4?

A24: A proposal's TA4 Integration Concept (part VI of Volume 1, described on BAA p. 23) should preferably include TAs 1, 2, and 3, but if that is impractical, should emphasize the TA(s) that have the most synergy with the particular approach being proposed. During program execution, the Government will choose whatever combinations of projects and TAs offer the greatest promise with respect to synergistic integration within TA4.

Q23: Would you expect to leverage the evolutionary work being done in the DHS DDOSD program (Dan Massey) to complement more revolutionary done for XD3?

A23: We are in communication with DHS. The interaction depends upon what the two programs produce.

Q22: What is the interest level in application specific (e.g. SIP) DDOS such as voice-video DOS or telephony DOS?

A22: Attacks against SIP are of interest. Strong proposals will have as broad a scope of applicability as possible.

Q21: Each TA describes or lists deficiencies or limitations of current art. Does a proposed solution need to address all such limitations to solve the problem in that area? Are all of the described deficiencies of equal importance?

A21: Strong proposals will address as many deficiencies as possible.

Q20: Can TA2 detect DDOS to decide when to maneuver, or should we assume TA3 will notify?

A20: TA2 can detect DDOS.

Q19: Is Phase 2 only a TA4 activity, or do TA1-3 continue in Phase 2?

A19: Technical areas 1-3 continue in Phase 2. TA4 is an optional activity that may or may not be exercised.

Q18: Can proposals use commercial cloud providers to provide a live-Internet testbed?

A18: Yes, but be clear about the costs.

Q17: Can proposals to one TA incorporate technology that is close to the scope of another TA in service of meeting their goals?

A17: To a limited extent, consider submitting two proposals if the approach has substantial components from both TAs and include a description of their synergy in your TA4 vision.

Q16: Is TA1 allowed to dynamically react to changing network conditions & traffic patterns to maintain dispersion, or would this be considered a maneuver (TA2)?

A16: TA1 may react to those network conditions.

Q15: Is this effort to protect secure networks like SIPR or protect Government usage across open commercial networks?

A15: Both.

Q14: Will any other contracting types other than the use of a CAS be considered, such as firm-fixed price?

A14: Yes, contract types are negotiable.

Q13: Can proposers reserve commercial rights, but agree to license to USG entities?

A13: Yes. Proposers can assert or provide the Government non-commercial licenses and later commercialize the intellectual property barring any export control or classification issues.

Q12: Are partial solutions in-scope (e.g. TA1 focusing on C2, as opposed to file transfer)?

A12: Yes. Proposals should clarify the scope of applicability. Proposals with relatively broad scope of applicability may be viewed more favorably.

Q11: Can TA1 consider approaches that control the physical network, such as utilizing bandwidth on demand from network?

A11: Yes.

Q10: Are deployable products in greater than 3 years of interest?

A10: Yes.

Q9: Can/should TA2 employ proactive maneuvers to complicate adversary planning?

A9: Yes.

Q8: Are offensive maneuvers (e.g. attack-base) in scope for TA2?

A8: No.

Q7: Is it in-scope to consider defenses against "indirect" attacks, such as targeting core infrastructure or nearby network elements?

A7: Yes.

Q6: Where do you expect defensive techniques to reside: within the WAN, enclaves, and/or endpoints?

A6: Predominately within enclaves and endpoints. WAN is ill-defined, so please submit a more clarified question.

Q5: Will the field exercises be conducted in a classified environment? Will it involve classified attack scenarios?

A5: Possibly, however, this has not yet been determined.

Q4: Is red teaming envisioned?

A4: Red teaming may be performed by Government partners as a part of field exercises.

Q3: For the end of phase experiments/demos, will the Government provide the experiment venue and/or testbed or is that the responsibility of the performers?

A3: The Government will provide the venue for field exercises.

Q2: Are protocols like IP anycast and source routing in scope?

A2: Yes, however, proposers must be more specific about the overall network context that is being addressed.

Q1: Can you explain the TA component experiments and system experiment milestones in the program schedule on page 13 of the BAA? What is the difference and why are some milestones only in Phase 1?

A1: This is a notional schedule only. The schedule assumes a performer may initially only be able to test components of its proposed system as opposed to the entire system.